**Amendments to the Claims**:

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A data generating apparatus, comprising:

a receiver that receives initial data and extracts first data and second data from the initial data;

a key generation data memory unit that holds the second data;

an encrypting key generation unit comprising a one-way function that generates an encrypting key from second data stored in the key generation data memory unit;

an encryptor that encrypts the first data with the encrypting key generated by the encrypting key generation unit;

a previous key memory unit that holds a previous key; and

a sender that generates final data including at least one of the result of encrypting by the encryptor and the second data stored in the key generation data memory unit,

wherein the encrypting key generation unit also uses the previous key stored in the previous key memory unit in generating the encrypting key.

2. (Canceled)

3. (Previously Presented) A data generating apparatus according to Claim 1, wherein the first data is a result of decrypting prescribed encrypted data.

4. (Previously Presented) A data generating apparatus according to Claim 1, wherein the first data is a signature for prescribed data.

5. (Previously Presented) A data generating apparatus according to Claim 1, wherein the encrypting key generation unit consists of a one-way function, and a result of

inputting the second data stored in the key generation data memory unit into the one-way function is the encrypting key.

6. (Previously Presented) A data generating apparatus according to Claim 1, further comprising:

the previous key encrypting key memory unit that holds a previous key encrypting key for encrypting the previous key; and

a previous key encryptor that encrypts the previous key with the previous key encrypting key stored in the previous key encrypting key memory unit.

7. (Original) A data generating apparatus according to Claim 1, wherein the encrypting performed by the encryptor is symmetric key encrypting.

8. (Previously Presented) A data generating apparatus according to Claim 1, wherein the encrypting performed by the encryptor is multiplication or division using the first data and the encrypting key generated by the encrypting key generation unit under a prescribed modulus number.

9. (Previously Presented) A data generating method comprising the steps of:

receiving initial data and extracting first data and second data from the initial data;

generating an encrypting key from the second data using a one-way function;

encrypting the first data with the encrypting key, the first data capable of being checked whether it includes a prescribed characteristic; and

generating final data including at least one of the second data and the encrypted first data,

wherein the encrypting key is also generated from a previous key stored in a previous key memory unit.

10. (Previously Presented) A data verifying apparatus, comprising:

a receiver that receives initial data and extracts first data and second data from the initial data;

a key generation data memory unit that holds the second data;

a decrypting key generation unit comprising a one-way function that generates a decrypting key from the second data stored in the key generation data memory unit;

a decryptor that decrypts the first data with the decrypting key generated by the decrypting key generation unit;

a verification unit that checks whether the first data decrypted by the decryptor has a prescribed characteristic and checks whether the decrypted first data is a result of decrypting prescribed data with a prescribed decrypting key; and

a previous key memory unit that holds a previous key, wherein the decrypting key generation unit, in generating a decrypting key, also uses the previous key stored in the previous key memory unit.

11-12. (Canceled)

13. (Previously Presented) A data verifying apparatus according to Claim 10, wherein the verification unit checks whether the data decrypted by the decryptor is a signature signed with a prescribed signature key.

14. (Previously Presented) A data verifying apparatus according to Claim 10, wherein the decrypting key generation unit consists of a one-way function, and a result of inputting the second data stored in the key generation data memory unit into the one-way function is the decrypting key.

15. (Previously Presented) A data verifying apparatus according to Claim 10, further comprising:

the previous key memory unit that stores an encrypted previous key;

a previous key decrypting key memory unit that stores a decrypting key for decrypting the encrypted previous key; and

a previous key decryptor that decrypts the encrypted previous key stored in the previous key memory unit with the decrypting key stored in the previous key decrypting key memory unit.

16. (Original) A data verifying apparatus according to Claim 10, wherein the decrypting performed by the decryptor is decrypting in symmetric key algorithm.

17. (Previously Presented) A data verifying apparatus according to Claim 10, wherein the decrypting performed by the decryptor is multiplication or division using the first data and the decrypting key generated by the decrypting key generation unit under a prescribed modulus number.

18. (Previously Presented) A data verifying method comprising the steps of:

receiving initial data and extracting first data and second data from the initial data;

generating a decrypting key from second data using a one-way function;

decrypting first data with the decrypting key; and

checking whether a result of decrypting includes a prescribed characteristic,

wherein the second data is also generated from a previous key stored in a previous key memory unit.

19. (Previously Presented) A data processing apparatus comprising a data generating apparatus and a data verifying apparatus for verifying the integrity of encrypted data generated by the data generating apparatus, wherein:

the data verifying apparatus further comprises:

a receiver that receives the encrypted data from the data generating apparatus;

a reference value data memory unit that holds first data;

a first key generation data memory unit that holds second data;

a decrypting key generation unit comprising a one-way function that generates a decrypting key from the second data stored in the first key generation data memory unit;

a decryptor that decrypts the encrypted data received from the data generating apparatus with the decrypting key generated by the decrypting key generation unit; and

a verification unit that checks whether the data decrypted by the decryptor has a prescribed relationship with respect to integrity with the first data stored in the reference value data memory unit, and

the data generating apparatus further comprises:

a receiver that receives the first data from the data verifying apparatus and that generates third data from the first data;

a second key generation data unit that holds fourth data;

an encrypting key generation unit that comprises a one-way function for generating an encrypting key from the fourth data stored in the second key generation data memory unit; and

an encryptor that encrypts the third data with the encrypting key generated by the encrypting key generation unit; and

a sender that sends the encrypted third data to the data verifying apparatus.

20. (Previously Presented) A data processing apparatus according to Claim 19, wherein the third data generated by the data generating apparatus is a result of decrypting with a prescribed decrypting key the first data from the data verifying apparatus, and the

verification unit of the data verifying apparatus checks whether the result of decrypting of encrypted data from the data generating apparatus is a result of decrypting the first data.

21. (Previously Presented) A data processing apparatus according to Claim 19, wherein the third data generated by the data generating apparatus is a signature generated by signing the first data sent from the data verifying apparatus with a prescribed signature key, and the verification unit of the data verifying apparatus checks if a result of decrypting the encrypted data sent from the data generating apparatus is a correct signature with respect to the first data.

22. (Previously Presented) A data processing apparatus according to Claim 19, wherein

the data generating apparatus further comprises:

a commitment random number memory unit that holds a random number; and

a commitment generation unit that generates a commitment from the random number stored in the commitment random number memory unit, and

the data verifying apparatus further comprises:

a commitment memory unit that stores the commitment sent from the data generating apparatus, wherein

the data generating apparatus sends, before it receives the first data from the data verifying apparatus, the commitment generated by the commitment generation unit to the data verifying apparatus,

the receiver also uses a random number stored in the commitment random number memory unit for generating the third data to be verified, and

the data verifying apparatus, when the verification unit performs checking, also uses the commitment stored in the commitment memory unit.

23. (Previously Presented) A data processing apparatus according to Claim 19, wherein the decrypting key generation unit of the data verifying apparatus consists of a one-way function, a result of entering the data stored in the first key generation data memory unit into the one-way function is the decrypting key, the encrypting key generation unit of the data generating apparatus is composed of the same one-way function as that of the decrypting key generation unit of the data verifying apparatus, and a result of entering the data stored in the second key generation data unit into the one-way function is the encrypting key.

24. (Previously Presented) A data processing apparatus according to Claim 19, wherein the data verifying apparatus further comprises:

a first previous key memory unit that holds a previous key, and

the decrypting key generation unit, when it is to generate the decrypting key, also uses the previous key stored in the first previous key memory unit, and

the data generating apparatus further comprises:

a second previous key memory unit that holds the previous key, and

the encrypting key generation unit, when it is to generate the encrypting key, also uses the previous key stored in the second previous key memory unit.

25. (Previously Presented) A data processing apparatus according to Claim 24, wherein:

the data generating apparatus further comprises:

a previous key encrypting key memory unit that stores a previous key encrypting key for encrypting the previous key; and

a previous key encryptor that encrypts the previous key with an encrypting key stored in the previous key encrypting key memory unit, and

the data verifying apparatus further comprises:

a previous key decrypting key memory unit that encrypts a previous key decrypting key for decrypting the encrypted previous key; and

a previous key decryptor for decrypting the encrypted previous key with a previous key decrypting key stored in the previous key decrypting key memory unit, wherein

the data generating apparatus encrypts the previous key stored in the second previous key memory unit with the previous key encryptor using the encrypting key stored in the previous key encrypting key memory unit, and sends the result to the data verifying apparatus, and

the data verifying apparatus decrypts the encrypted previous key sent from the data generating apparatus with the previous key decryptor using the decrypting key stored in the previous key decrypting key memory unit, and stores the result in the first previous key memory unit.

26. (Previously Presented) A data processing apparatus according to Claim 19, wherein

the data verifying apparatus sends data held in the first key generation data memory unit to the data generating apparatus, and

the data generating apparatus stores the data sent from the data verifying apparatus in the second key generation data memory unit for use in generation of the encrypting key.

27. (Previously Presented) A data processing apparatus according to Claim 19, wherein

the data generating apparatus sends the fourth data held in the second key generation data memory unit to the data verifying apparatus, and the data verifying apparatus

stores the fourth data from the data generating apparatus in the first key generation data unit for use in generation of the decrypting key.

28. (Original) A data processing apparatus according to Claim 19, wherein the encrypting performed by the encryptor is the encrypting using a symmetric key algorithm with the encrypting key, and the decrypting performed by the decryptor is the decrypting using a symmetric key algorithm with the decrypting key.

29. (Previously Presented) A data processing apparatus according to Claim 19, wherein the encrypting performed by the encryptor is multiplication or division using the third data and the encrypting key under a prescribed modulus number, and the decrypting performed by the decryptor is multiplication or division using the encrypted data from the data generating apparatus by the decrypting key under the same modulus number used in the encryptor.

30. (Previously Presented) A data processing apparatus, comprising:

a first device comprising a first data memory means and an encrypting means including a one-way function; and

a second device comprising a second data memory means, a decrypting means including a one-way function and a verifying means,

wherein the first device encrypts prescribed data received from the second device to be verified with the encrypting means on the basis of first data stored in the first data memory means, and the second device decrypts the encrypted prescribed data received from the first device with the decrypting means on the basis of second data stored in the second data memory means, verifies the integrity of the result of decrypting with the verifying means, and, if the data is successfully verified, authenticates the identity between the first data stored in the first data memory means and the second data stored in the second data memory means.

31. (Currently Amended) A data processing apparatus according to Claim 30, wherein at least part of the ~~data first~~first data stored in the first data memory means is the prescribed data received from the second device.

32. (Previously Presented) A data processing apparatus according to Claim 30, wherein at least part of the second data stored in the second data memory means is the encrypted prescribed data received from the first device.